UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/346,559	06/30/1999	DAVID GOLDBERG	D/99176	2589

47374 7590 03/10/2008
CASCADIA INTELLECTUAL PROPERTY
500 UNION STREET
SUITE 1005
SEATTLE, WA 98101

EXAMINER	
THOMPSON, JAMES A	

ART UNIT	PAPER NUMBER
2625	

MAIL DATE	DELIVERY MODE
03/10/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte DAVID GOLDBERG, WILLIAM J. RUCKLIDGE,
and JAMES D. THORNTON

Appeal 2007-3563
Application 09/346,559
Technology Center 2600

Decided: March 10, 2008

Before JOSEPH F. RUGGIERO, ROBERT E. NAPPI, and JOHN A. JEFFERY, *Administrative Patent Judges*.

JEFFERY, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellants appeal under 35 U.S.C. § 134 from the Examiner's rejection of claims 1-23. We have jurisdiction under 35 U.S.C. § 6(b). We reverse.

STATEMENT OF THE CASE

Appellants invented digital methods for authenticating hardcopy documents. Initially, a scanned representation of the hardcopy document is recorded in memory at a selected resolution. Lossy compression image data is generated and an authentication token is produced. The scanned representation of the hardcopy document is arranged in memory with a digital encoding of the authentication data for rendering at a printer a signed hardcopy document.[1] Claim 1 is illustrative with the key disputed limitation emphasized:

> 1. A method for authenticating a hardcopy document, comprising the steps of:
>
> recording in a memory a scanned representation of the hardcopy document at a selected resolution;
>
> generating lossy compressed image data with the scanned representation of the hardcopy document;
>
> producing an authentication token with the lossy compressed image data; the authentication token including one of encrypted image data and hashed encrypted image data; the hashed encrypted image data including the lossy compressed image data and an encrypted hash of the lossy compressed image data; and
>
> arranging in the memory the scanned representation of the hardcopy document with a digital *encoding* of the authentication token for rendering at a printer a signed and authenticated hardcopy document.

[1] *See generally* Spec. 3:5-24.

The Examiner relies on the following prior art references to show unpatentability:

Merkle	US 5,157,726	Oct. 20, 1992
Zdybel	US 5,486,686	Jan. 23, 1996
Squilla	US 5,898,779	Apr. 27, 1999 (filed Apr. 14, 1997)
Curry	US 5,946,103	Aug. 31, 1999 (filed Jan. 29, 1998)
Walker	US 6,111,953	Aug. 29, 2000 (filed May 21, 1997)

1. Claims 1-3, 5, 7, 8, 12, 13, and 21-23 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Squilla.
2. Claim 4 stands rejected under 35 U.S.C. § 103(a) as unpatentable over Squilla and Merkle.
3. Claims 6 and 9-11 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Squilla and Curry.
4. Claims 14-17 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Squilla and Zdybel.
5. Claims 18-20 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Squilla and Walker.

Rather than repeat the arguments of Appellants or the Examiner, we refer to the Briefs and the Answer for their respective details. In this decision, we have considered only those arguments actually made by Appellants. Arguments which Appellants could have made but did not make in the Briefs have not been considered and are deemed to be waived. *See* 37 C.F.R. § 41.37(c)(1)(vii).

The Anticipation Rejection

We first consider the Examiner's rejection of claims 1-3, 5, 7, 8, 12, 13, and 21-23 under 35 U.S.C. § 102(e) as being anticipated by Squilla. The Examiner has indicated how the claimed invention is deemed to be fully met by the disclosure of Squilla (Ans. 3-6). Regarding independent claims 1 and 21, Appellants argue that Squilla does not disclose rendering at a printer a signed hardcopy document as claimed (App. Br. 11; Reply Br. 5-6). Appellants also argue that Squilla fails to disclose an authentication token with hashed encrypted image data including (1) lossy compressed image data, and (2) an encrypted hash of the lossy compressed image data (App. Br. 12; Reply Br. 7).

Additionally, Appellants argue that Squilla does not arrange in memory a scanned representation of the hardcopy document with a digital *encoding* of the authentication token as claimed. Although Appellants acknowledge that Squilla creates a digital signature by selecting, compressing, hashing a region of interest, and then encrypting the hash using a private key, the digital signature is appended to a digital image file for storage. Such a process, Appellants contend, does not *encode* the compressed, hashed, and encrypted image data in the manner claimed (Reply Br. 6-7; emphasis added).

The Examiner acknowledges that while Squilla's primary embodiment may operate solely in digital formats, the reference nonetheless discloses embodiments that utilize a scanner to input image data into the system and a printer for printing hardcopy documents (Ans. 13-14). The Examiner also refers to the process detailed in column 8, lines 34 through 51 of Squilla for teaching that the authentication token includes lossy compressed image data and an encrypted hash of that data (Ans. 14-15).

ISSUE

The key issue before us is whether Appellants have shown that the Examiner erred in finding Squilla discloses all limitations of independent claims 1 and 21. Specifically, the issue turns on whether Squilla expressly or inherently discloses the following disputed limitations:

(1) rendering at a printer a signed hardcopy document;

(2) producing an authentication token with hashed encrypted image data including (a) lossy compressed image data, and (b) an encrypted hash of the lossy compressed image data; and

(3) arranging in memory a scanned representation of the hardcopy document with a digital encoding of the authentication token, as claimed.

FINDINGS OF FACT

Squilla discloses a system that authenticates images captured by a digital camera. A key feature of Squilla's system is that it allows the photographer to choose a region of interest of the image for authentication in lieu of the entire image. As a result, subsequent authentication processing (i.e., hashing and encryption) is confined to the selected region of interest, thus reducing power requirements (Squilla, col. 2, l. 59 - col. 3, l. 34).

The encryption procedure in Squilla most relevant to this appeal is shown in Figure 7. As the figure illustrates, after certain region(s) of a captured image are selected, they are compressed using a lossy compression scheme (Squilla; col. 8, ll. 20-44; Fig. 7 (Step 92)). The compressed data is then hashed.[2] Then, "photographer's information"[3] is appended to this hashed file, and the data is encrypted to create the digital signature. The digital signature is then appended to the digital image file and stored. The resulting output file format is shown in Figure 4 (Squilla, Fig. 7, Steps 74, 78, and 80; col. 8, ll. 44-51; col. 7, ll. 55-58; col. 5, ll. 41-53; Fig. 4).

In addition to digital cameras, this authentication process can also be used in conjunction with a scanner or scanning service (Squilla, col. 9, ll. 15-26).

PRINCIPLES OF LAW

Anticipation is established only when a single prior art reference discloses, expressly or under the principles of inherency, each and every element of a claimed invention as well as disclosing structure which is capable of performing the recited functional limitations. *RCA Corp. v. Applied Digital Data Systems, Inc.*, 730 F.2d 1440, 1444 (Fed. Cir. 1984); *W.L. Gore and Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540, 1554 (Fed. Cir. 1983).

[2] Typical one-way hash functions produce a fixed-size digital file (e.g., 20 bytes) for a digital input file of any size. The hashed value serves as a fingerprint of the image while significantly reducing the size of the data that is subsequently encrypted. *See generally* Squilla, col. 7, ll. 2-20.

[3] "Photographer's information" is additional information inputted by the user to include along with the image. This information can include, among other things, time of day, exposure settings, name of the photographer, etc. (Squilla, col. 5, l. 60 - col. 6, l. 5).

Claim terms are "generally given their ordinary and customary meaning." *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc). And "the ordinary and customary meaning of a claim term is the meaning that the term would have to a person of ordinary skill in the art." *Id.* at 1313.

To determine the ordinary meaning of commonly understood words, it is entirely appropriate to cite a dictionary definition. *Agfa Corp. v. Creo Products, Inc.*, 451 F.3d 1366, 1376 (Fed. Cir. 2006). Nevertheless, any reliance on dictionaries must nevertheless accord with the intrinsic evidence: the claims, Specification, and the prosecution history. *Free Motion Fitness, Inc. v. Cybex Int'l, Inc.*, 423 F.3d 1343, 1348 (Fed. Cir. 2005) (internal citations omitted).

In rejecting claims under 35 U.S.C. § 103, it is incumbent upon the Examiner to establish a factual basis to support the legal conclusion of obviousness. *See In re Fine*, 837 F.2d 1071, 1073 (Fed. Cir. 1988). In so doing, the Examiner must make the factual determinations set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 17 (1966). If the Examiner's burden is met, the burden then shifts to the Appellants to overcome the prima facie case with argument and/or evidence. Obviousness is then determined on the basis of the evidence as a whole and the relative persuasiveness of the arguments. *See In re Oetiker*, 977 F.2d 1443, 1445 (Fed. Cir. 1992).

ANALYSIS

At the outset, we agree with the Examiner that Squilla teaches that a scanner can be used (Squilla, col. 9, ll. 15-26). Moreover, while the reference is short on specifics, Squilla nonetheless nominally suggests printing (Squilla, col. 8, l. 61).

We further note that independent claims 1 and 21 call for producing an authentication token that includes *one of* (1) encrypted image data, and (2) hashed encrypted image data. Therefore, to anticipate this limitation only one alternative need be disclosed -- a fact fully supported by the Specification.[4] As a result, Appellants' arguments pertaining to the specific details of alternative (2) (i.e., the hashed encrypted image data includes both (a) lossy compressed image data, and (b) an encrypted hash of the lossy compressed image data) are not dispositive to the issue of whether Squilla anticipates the claims, as we must determine whether Squilla also discloses alternative (1) (i.e., whether the token includes encrypted image data).

In our view, the digital signature ("authentication token") created at Step 78 in Figure 7 fully meets alternative (1) above. That is, the digital signature includes "encrypted image data" in the form of the encrypted hash and appended photographer's information. While we agree with Appellants that Squilla does not anticipate alternative (2) since the lossy compressed

[4] According to the Specification, "[t]he authentication token generator 114 produces the authentication token 122 by *either* encrypting the compressed image data 112 (i.e., encrypted image data) *or* by encrypting a hash of the compressed image data 112. *When a hash of the compressed image data 112 is encrypted*, the authentication token 122 includes both the encrypted hash of the compressed image data and the compressed image data 112 (i.e., hashed encrypted image data)." (Spec. 8:1-6; emphasis added).

image data is not included *in addition to* the encrypted hash of this lossy encrypted image data, we nonetheless find alternative (1) fully met by Squilla.

However, we do not find that Squilla digitally *encodes* the authentication token for rendering at a printer a signed and authenticated hardcopy document as claimed. At best, Squilla merely *appends* the digital signature (token) to the digital image file as shown in Step 80 of Figure 7 to produce an output file shown in Figure 4. Simply put, merely appending the token to a file is not *encoding* the token itself -- an essential feature recited in independent claims 1 and 21.

The term "encode" is defined as "*convert* into a coded form"[5] and "[t]o *convert* signals or data into a desired (usually digital) form".[6] The key term in these definitions is "convert": a term that indicates that some sort of conversion or transformation of the data occurs as a result of the encoding process. Additionally, "encoding" is defined as "[t]he *translation,* either by a machine or by a human operator, of a spoken or written language into digital code."[7] Based on the ordinary and customary meaning of the term "encoding," and interpreting the term in light of the Specification,[8] we find

[5] The Compact Oxford English Dictionary of Current English, *available at* http://www.askoxford.com/concise_oed/encode?view=uk (last visited Feb. 29, 2008) (emphasis added).

[6] Stan Gibilisco, *The Illustrated Dictionary of Electronics,* 8th ed., 2001 (emphasis added).

[7] *Id.* (emphasis added).

[8] *See Phillips v. AWH Corp.,* 415 F.3d 1303, 1316 (Fed. Cir. 2005) (en banc) ("The construction that stays true to the claim language and most naturally

that merely appending the token to a digital file as in Squilla falls short of encoding the token itself.

For the foregoing reasons, we will not sustain the Examiner's rejection of independent claims 1 and 21 or dependent claims 3-17, 22, and 23 for similar reasons.

The Obviousness Rejections

Regarding the obviousness rejections of claims 4, 6, 9-11, and 14-20, since we find that the disclosures of the cited secondary references do not cure the deficiencies noted above with respect to Squilla, namely encoding the authentication token itself, the obviousness rejections are also not sustained for the reasons noted above.

CONCLUSIONS OF LAW

We conclude that the Examiner erred in finding that Squilla arranges in memory a scanned representation of the hardcopy document with a digital encoding of the authentication token, as recited in independent claims 1 and 21. We further conclude that since the cited secondary references do not cure this deficiency, the Examiner's obviousness rejections are likewise in error.

aligns with the patent's description of the invention will be, in the end, the correct construction.") (citations omitted).

DECISION

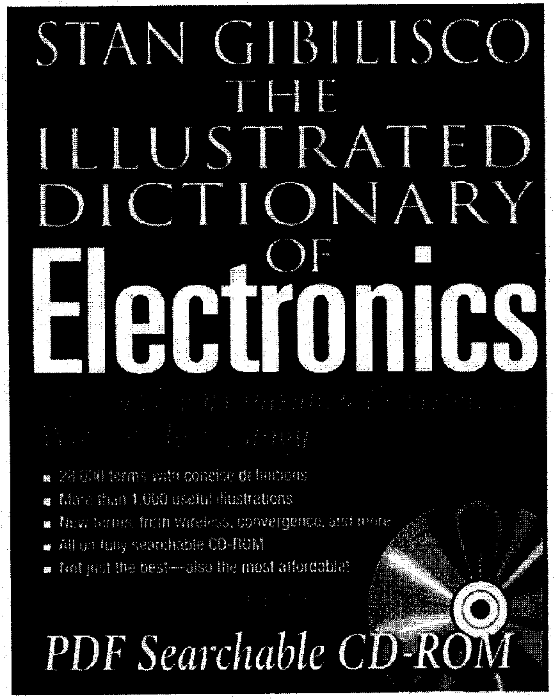
We have not sustained the Examiner's rejections with respect to any of the claims on appeal. Therefore, the Examiner’s decision rejecting claims 1-23 is reversed.

REVERSED

eld

CASCADIA INTELLECTUAL PROPERTY
500 UNION STREET SUITE 1005
SEATLE, WA 98101

EVIDENCE APPENDIX



STAN GIBILISCO
THE
ILLUSTRATED
DICTIONARY
OF
Electronics

[illegible]

[illegible]

- 28,000 terms with concise definitions
- More than 1,000 useful illustrations
- New terms from wireless, convergence, and more
- All on fully searchable CD-ROM
- Not just the best—also the most affordable!

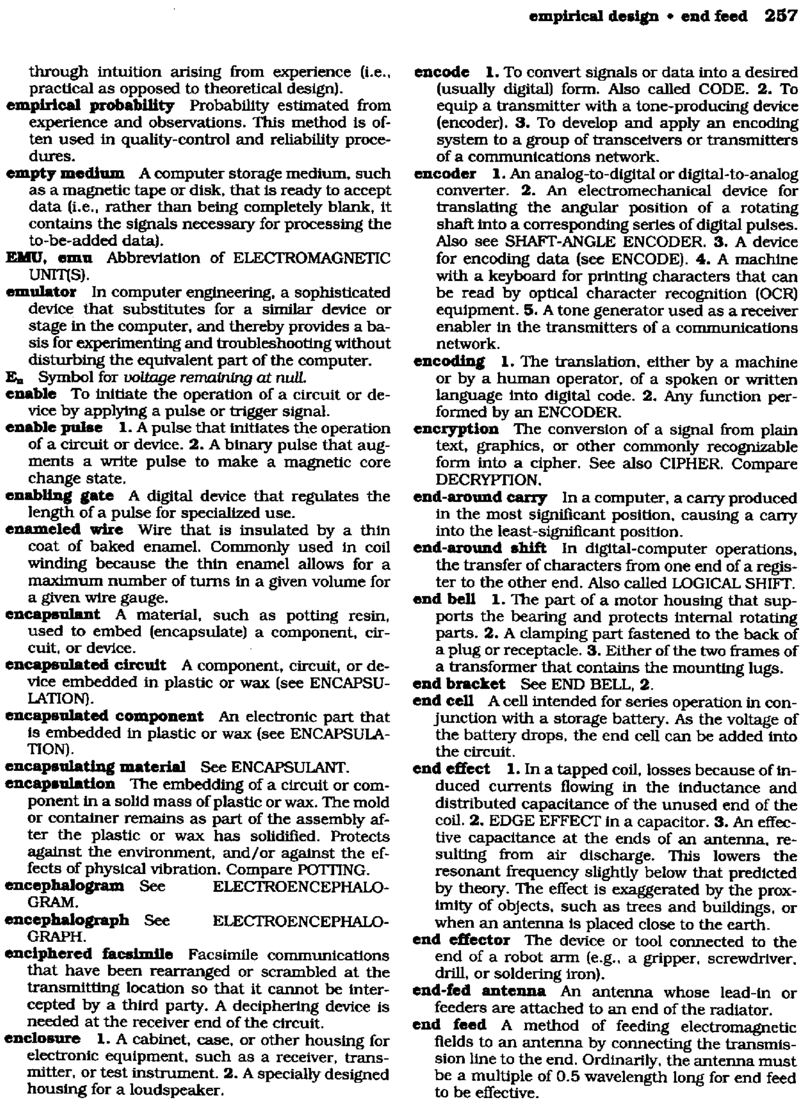
PDF Searchable CD-ROM

McGraw-Hill

A Division of The McGraw-Hill Companies

0-07-138966-0
The material in this eBook also appears in the print version of this title: 0-07-137236-9.

DOI: 10.1036/0071389660



through intuition arising from experience (i.e., practical as opposed to theoretical design).

empirical probability Probability estimated from experience and observations. This method is often used in quality-control and reliability procedures.

empty medium A computer storage medium, such as a magnetic tape or disk, that is ready to accept data (i.e., rather than being completely blank, it contains the signals necessary for processing the to-be-added data).

EMU, emu Abbreviation of ELECTROMAGNETIC UNIT(S).

emulator In computer engineering, a sophisticated device that substitutes for a similar device or stage in the computer, and thereby provides a basis for experimenting and troubleshooting without disturbing the equivalent part of the computer.

E_n Symbol for *voltage remaining at null.*

enable To initiate the operation of a circuit or device by applying a pulse or trigger signal.

enable pulse **1.** A pulse that initiates the operation of a circuit or device. **2.** A binary pulse that augments a write pulse to make a magnetic core change state.

enabling gate A digital device that regulates the length of a pulse for specialized use.

enameled wire Wire that is insulated by a thin coat of baked enamel. Commonly used in coil winding because the thin enamel allows for a maximum number of turns in a given volume for a given wire gauge.

encapsulant A material, such as potting resin, used to embed (encapsulate) a component, circuit, or device.

encapsulated circuit A component, circuit, or device embedded in plastic or wax (see ENCAPSULATION).

encapsulated component An electronic part that is embedded in plastic or wax (see ENCAPSULATION).

encapsulating material See ENCAPSULANT.

encapsulation The embedding of a circuit or component in a solid mass of plastic or wax. The mold or container remains as part of the assembly after the plastic or wax has solidified. Protects against the environment, and/or against the effects of physical vibration. Compare POTTING.

encephalogram See ELECTROENCEPHALOGRAM.

encephalograph See ELECTROENCEPHALOGRAPH.

enciphered facsimile Facsimile communications that have been rearranged or scrambled at the transmitting location so that it cannot be intercepted by a third party. A deciphering device is needed at the receiver end of the circuit.

enclosure **1.** A cabinet, case, or other housing for electronic equipment, such as a receiver, transmitter, or test instrument. **2.** A specially designed housing for a loudspeaker.

encode **1.** To convert signals or data into a desired (usually digital) form. Also called CODE. **2.** To equip a transmitter with a tone-producing device (encoder). **3.** To develop and apply an encoding system to a group of transceivers or transmitters of a communications network.

encoder **1.** An analog-to-digital or digital-to-analog converter. **2.** An electromechanical device for translating the angular position of a rotating shaft into a corresponding series of digital pulses. Also see SHAFT-ANGLE ENCODER. **3.** A device for encoding data (see ENCODE). **4.** A machine with a keyboard for printing characters that can be read by optical character recognition (OCR) equipment. **5.** A tone generator used as a receiver enabler in the transmitters of a communications network.

encoding **1.** The translation, either by a machine or by a human operator, of a spoken or written language into digital code. **2.** Any function performed by an ENCODER.

encryption The conversion of a signal from plain text, graphics, or other commonly recognizable form into a cipher. See also CIPHER. Compare DECRYPTION.

end-around carry In a computer, a carry produced in the most significant position, causing a carry into the least-significant position.

end-around shift In digital-computer operations, the transfer of characters from one end of a register to the other end. Also called LOGICAL SHIFT.

end bell **1.** The part of a motor housing that supports the bearing and protects internal rotating parts. **2.** A clamping part fastened to the back of a plug or receptacle. **3.** Either of the two frames of a transformer that contains the mounting lugs.

end bracket See END BELL, **2**.

end cell A cell intended for series operation in conjunction with a storage battery. As the voltage of the battery drops, the end cell can be added into the circuit.

end effect **1.** In a tapped coil, losses because of induced currents flowing in the inductance and distributed capacitance of the unused end of the coil. **2.** EDGE EFFECT in a capacitor. **3.** An effective capacitance at the ends of an antenna, resulting from air discharge. This lowers the resonant frequency slightly below that predicted by theory. The effect is exaggerated by the proximity of objects, such as trees and buildings, or when an antenna is placed close to the earth.

end effector The device or tool connected to the end of a robot arm (e.g., a gripper, screwdriver, drill, or soldering iron).

end-fed antenna An antenna whose lead-in or feeders are attached to an end of the radiator.

end feed A method of feeding electromagnetic fields to an antenna by connecting the transmission line to the end. Ordinarily, the antenna must be a multiple of 0.5 wavelength long for end feed to be effective.